FIG. 1

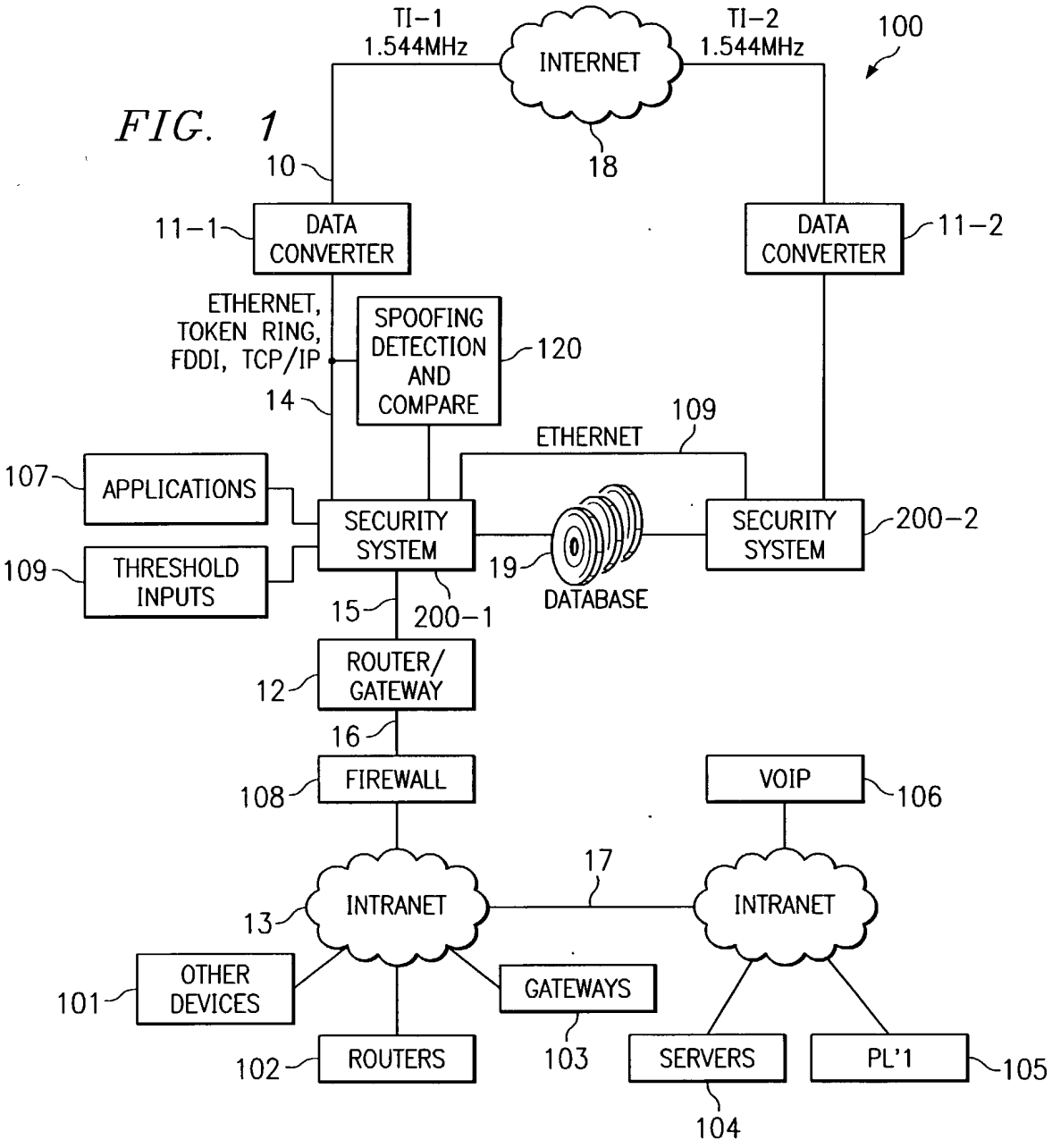

TI-1
1.544MHz
INTERNET
TI-2
1.544MHz
100
18
10
11-1
DATA CONVERTER
DATA CONVERTER
11-2
ETHERNET, TOKEN RING, FDDI, TCP/IP
SPOOFING DETECTION AND COMPARE
120
14
109
ETHERNET
107
APPLICATIONS
SECURITY SYSTEM
SECURITY SYSTEM
200-2
109
THRESHOLD INPUTS
19
DATABASE
15
200-1
ROUTER/ GATEWAY
12
16
108
FIREWALL
VOIP
106
17
INTRANET
INTRANET
13
OTHER DEVICES
101
GATEWAYS
103
ROUTERS
102
SERVERS
PL'1
105
104

FIG. 2

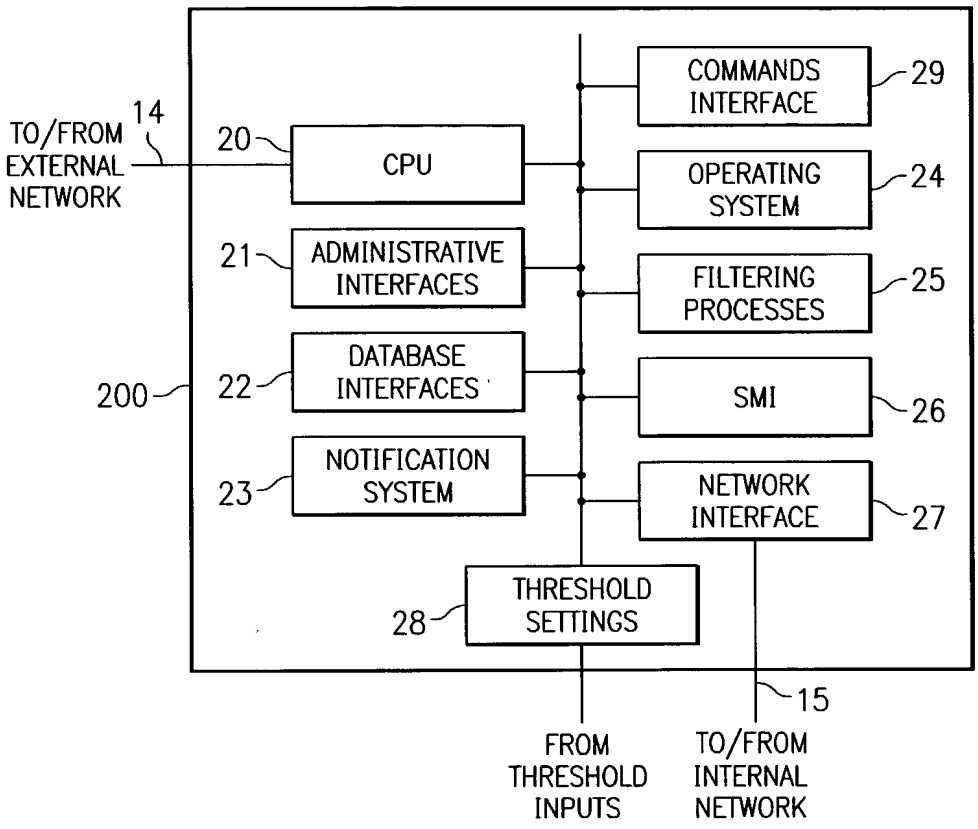
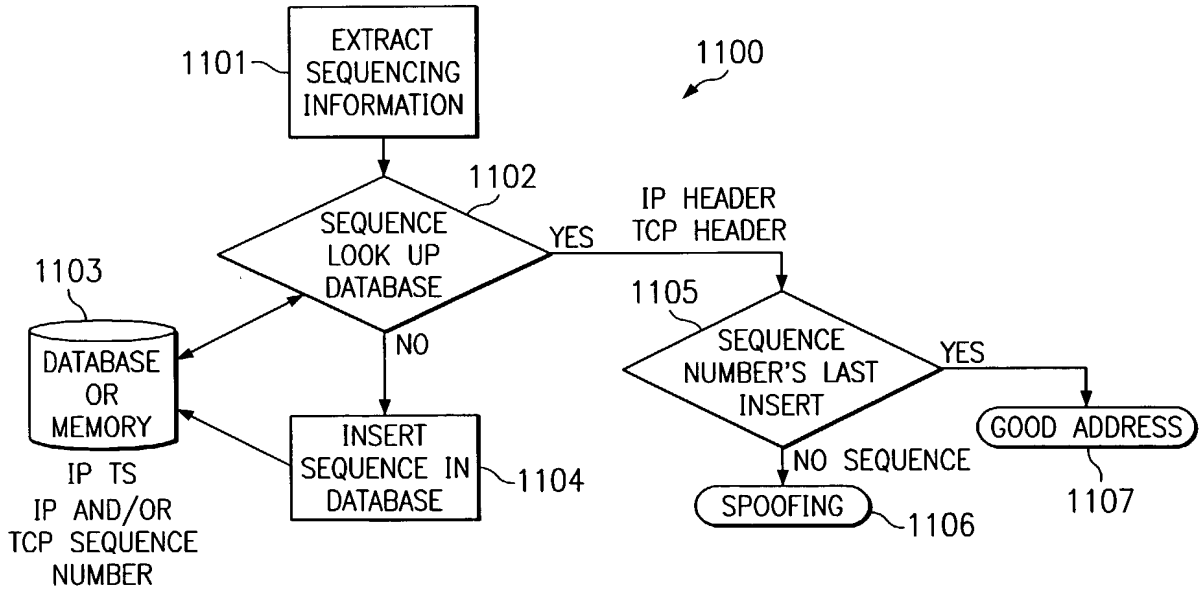

TO/FROM EXTERNAL NETWORK
14
20
CPU
21
ADMINISTRATIVE INTERFACES
22
DATABASE INTERFACES
200
23
NOTIFICATION SYSTEM
28
THRESHOLD SETTINGS
COMMANDS INTERFACE
29
OPERATING SYSTEM
24
FILTERING PROCESSES
25
SMI
26
NETWORK INTERFACE
27
15
FROM THRESHOLD INPUTS
TO/FROM INTERNAL NETWORK

FIG. 11


1100
1101
EXTRACT SEQUENCING INFORMATION
1102
SEQUENCE LOOK UP DATABASE
YES
IP HEADER TCP HEADER
NO
1103
DATABASE OR MEMORY
IP TS
IP AND/OR TCP SEQUENCE NUMBER
INSERT SEQUENCE IN DATABASE
1104
1105
SEQUENCE NUMBER'S LAST INSERT
YES
GOOD ADDRESS
1107
NO SEQUENCE
SPOOFING
1106

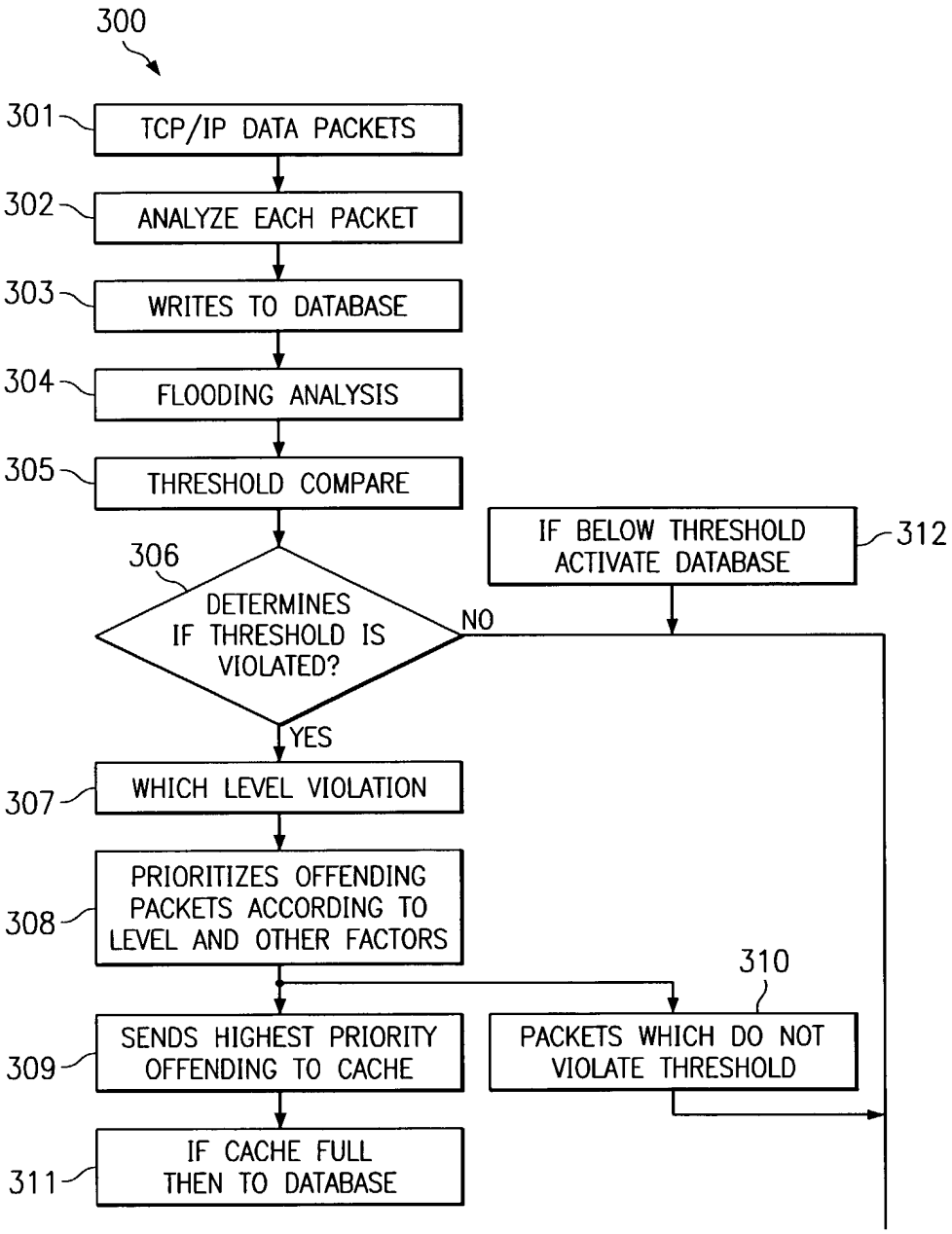

300
301
TCP/IP DATA PACKETS
302
ANALYZE EACH PACKET
303
WRITES TO DATABASE
304
FLOODING ANALYSIS
305
THRESHOLD COMPARE
306
DETERMINES IF THRESHOLD IS VIOLATED?
NO
YES
IF BELOW THRESHOLD ACTIVATE DATABASE
312
307
WHICH LEVEL VIOLATION
308
PRIORITIZES OFFENDING PACKETS ACCORDING TO LEVEL AND OTHER FACTORS
310
309
SENDS HIGHEST PRIORITY OFFENDING TO CACHE
PACKETS WHICH DO NOT VIOLATE THRESHOLD
311
IF CACHE FULL THEN TO DATABASE

FIG. 3

FIG. 4

0	1	2	3	4	5	6
MAIN POSIX PTS 2	IP1	CRUNCH	DETER CHOKE	WISH SUM LOWER	2 DATABASE FILTERS	SYNCH SHARED RESOURCES

FIG. 5

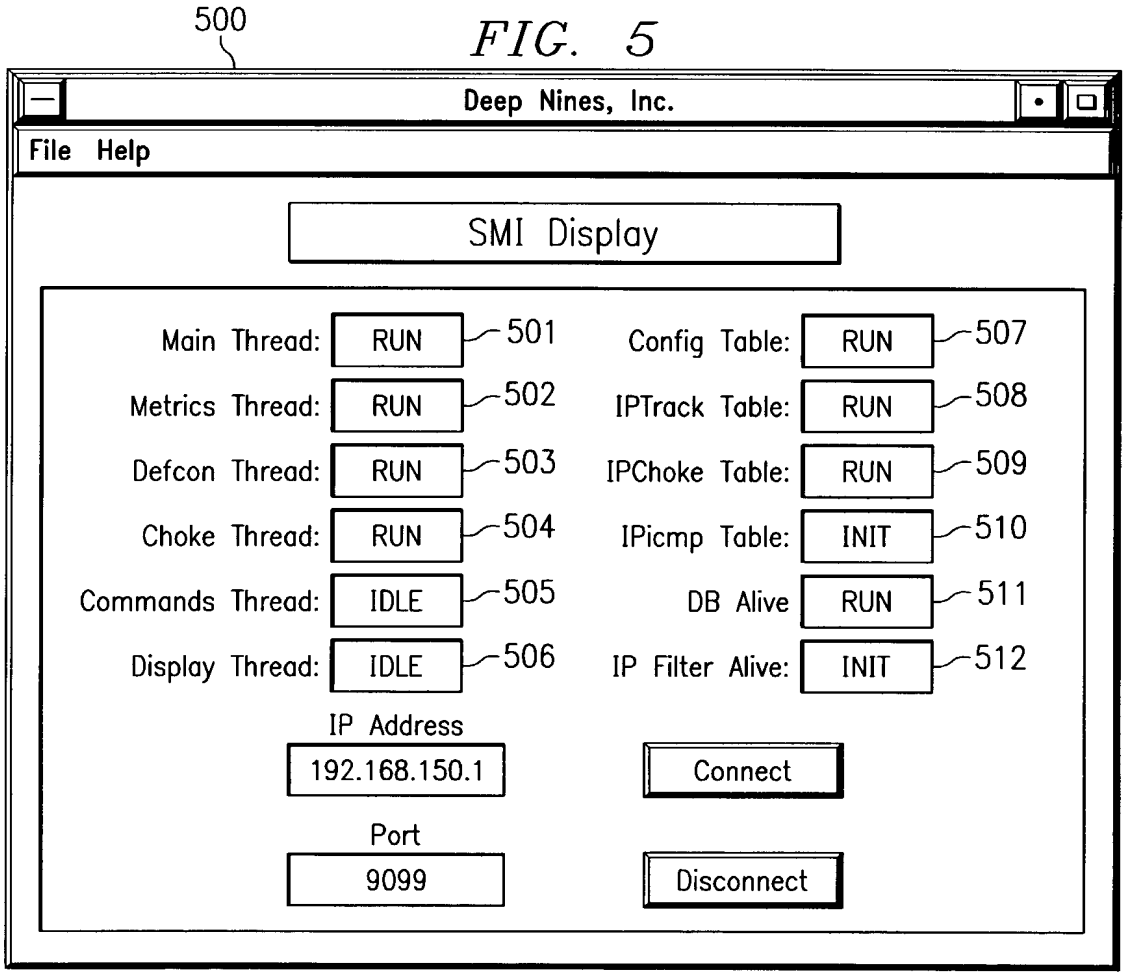


FIG. 6

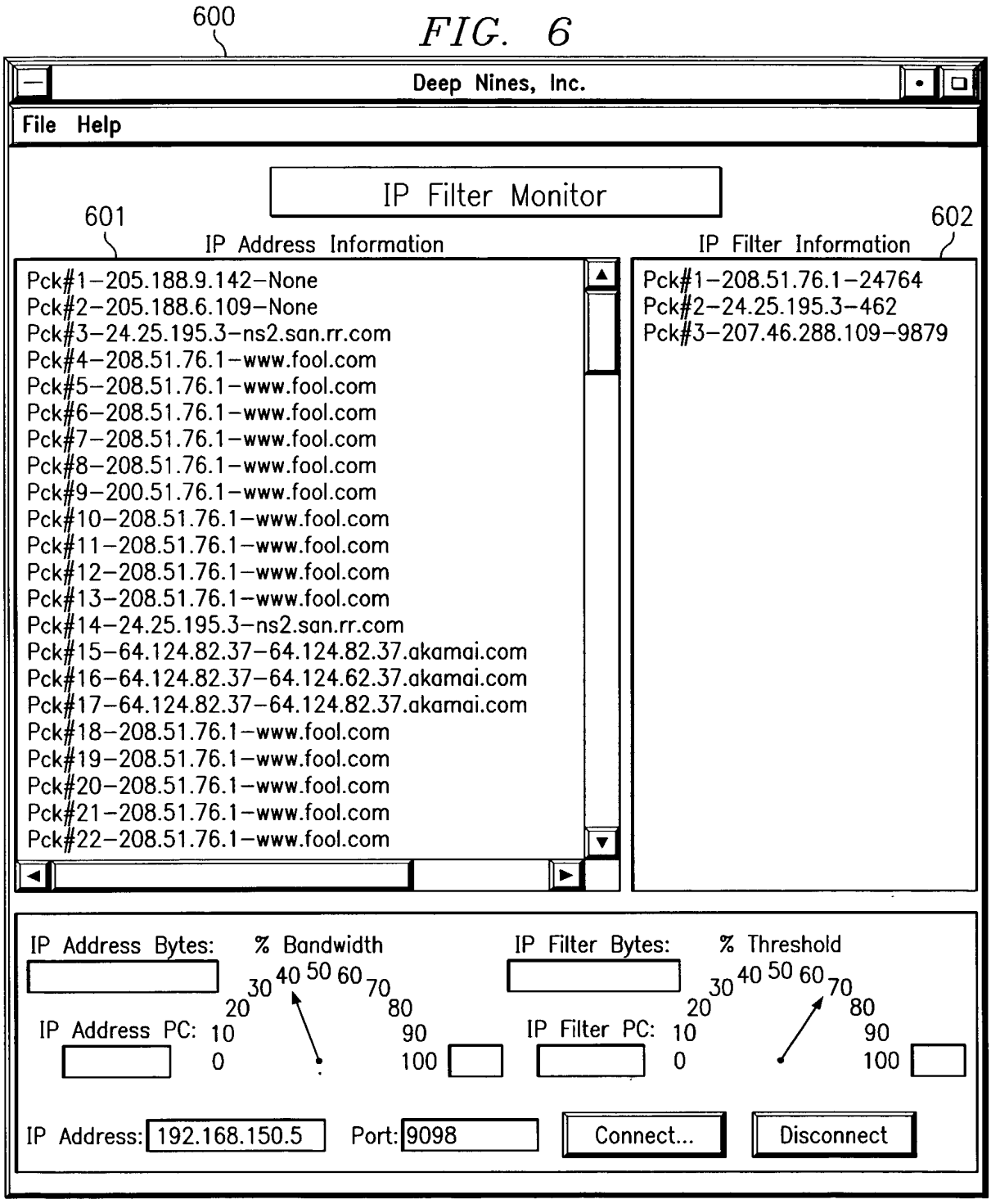
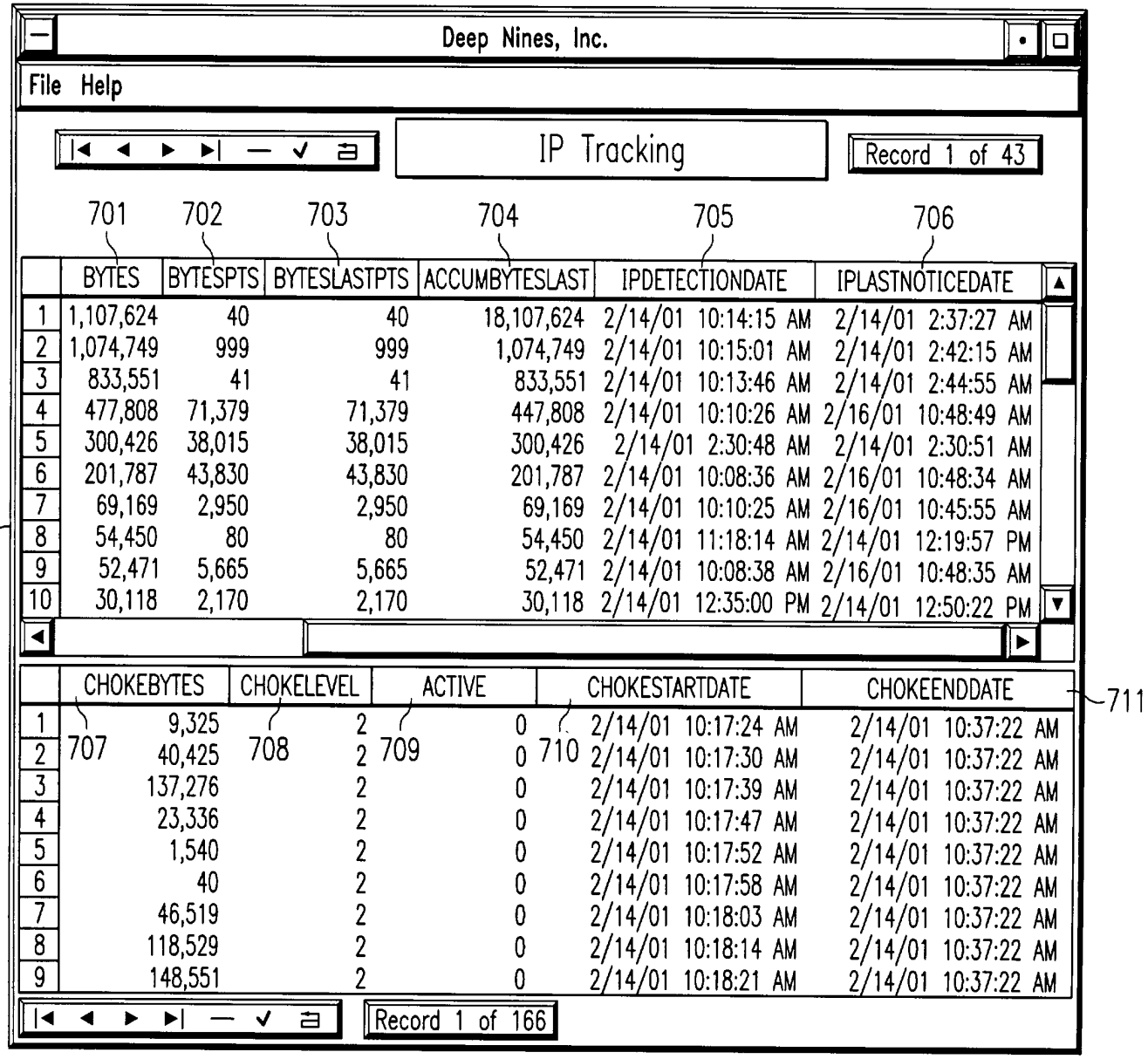

600
Deep Nines, Inc.
File Help
IP Filter Monitor
601
IP Address Information
602
IP Filter Information
Pck#1-205.188.9.142-None
Pck#2-205.188.6.109-None
Pck#3-24.25.195.3-ns2.san.rr.com
Pck#4-208.51.76.1-www.fool.com
Pck#5-208.51.76.1-www.fool.com
Pck#6-208.51.76.1-www.fool.com
Pck#7-208.51.76.1-www.fool.com
Pck#8-208.51.76.1-www.fool.com
Pck#9-200.51.76.1-www.fool.com
Pck#10-208.51.76.1-www.fool.com
Pck#11-208.51.76.1-www.fool.com
Pck#12-208.51.76.1-www.fool.com
Pck#13-208.51.76.1-www.fool.com
Pck#14-24.25.195.3-ns2.san.rr.com
Pck#15-64.124.82.37-64.124.82.37.akamai.com
Pck#16-64.124.82.37-64.124.62.37.akamai.com
Pck#17-64.124.82.37-64.124.82.37.akamai.com
Pck#18-208.51.76.1-www.fool.com
Pck#19-208.51.76.1-www.fool.com
Pck#20-208.51.76.1-www.fool.com
Pck#21-208.51.76.1-www.fool.com
Pck#22-208.51.76.1-www.fool.com
Pck#1-208.51.76.1-24764
Pck#2-24.25.195.3-462
Pck#3-207.46.288.109-9879
IP Address Bytes:
% Bandwidth
IP Filter Bytes:
% Threshold
0 10 20 30 40 50 60 70 80 90 100
IP Address PC:
IP Filter PC:
IP Address: 192.168.150.5
Port: 9098
Connect...
Disconnect

FIG. 7



58895-P001CP1CP1-10111610

800

FIG. 8

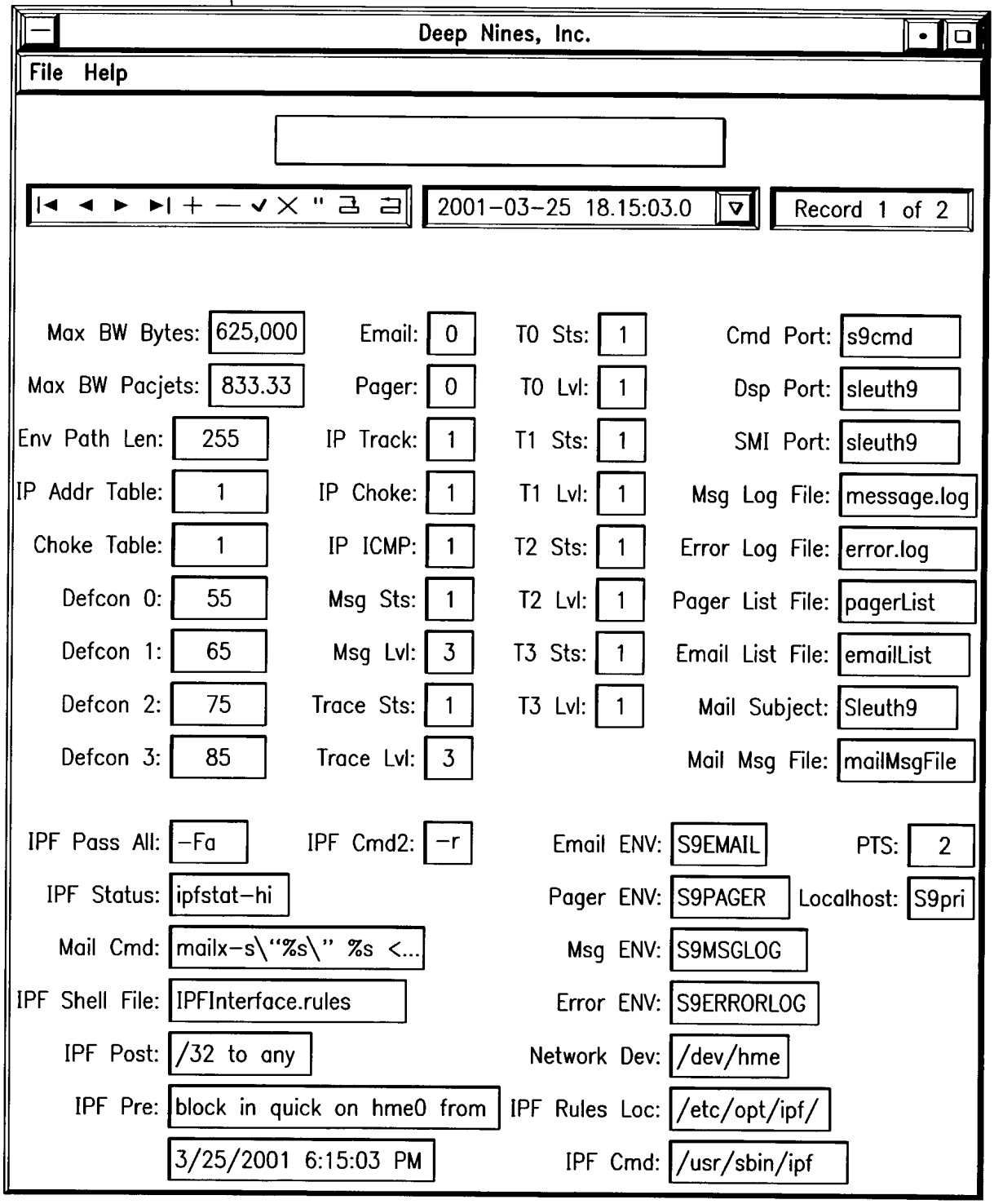

Deep Nines, Inc.
File Help
2001-03-25 18.15:03.0
Record 1 of 2
Max BW Bytes: 625,000
Email: 0
T0 Sts: 1
Cmd Port: s9cmd
Max BW Pacjets: 833.33
Pager: 0
T0 Lvl: 1
Dsp Port: sleuth9
Env Path Len: 255
IP Track: 1
T1 Sts: 1
SMI Port: sleuth9
IP Addr Table: 1
IP Choke: 1
T1 Lvl: 1
Msg Log File: message.log
Choke Table: 1
IP ICMP: 1
T2 Sts: 1
Error Log File: error.log
Defcon 0: 55
Msg Sts: 1
T2 Lvl: 1
Pager List File: pagerList
Defcon 1: 65
Msg Lvl: 3
T3 Sts: 1
Email List File: emailList
Defcon 2: 75
Trace Sts: 1
T3 Lvl: 1
Mail Subject: Sleuth9
Defcon 3: 85
Trace Lvl: 3
Mail Msg File: mailMsgFile
IPF Pass All: -Fa
IPF Cmd2: -r
Email ENV: S9EMAIL
PTS: 2
IPF Status: ipfstat-hi
Pager ENV: S9PAGER
Localhost: S9pri
Mail Cmd: mailx-s\"%s\" %s <...
Msg ENV: S9MSGLOG
IPF Shell File: IPFInterface.rules
Error ENV: S9ERRORLOG
IPF Post: /32 to any
Network Dev: /dev/hme
IPF Pre: block in quick on hme0 from
IPF Rules Loc: /etc/opt/ipf/
3/25/2001 6:15:03 PM
IPF Cmd: /usr/sbin/ipf

FIG. 9

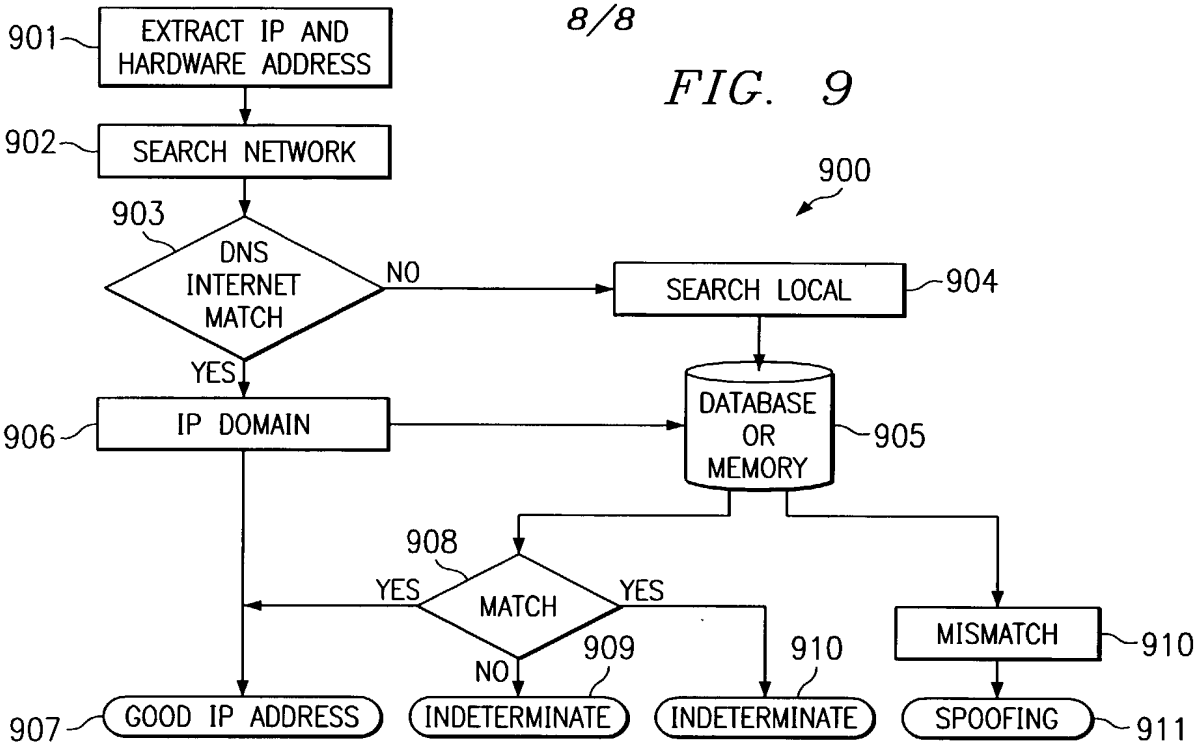
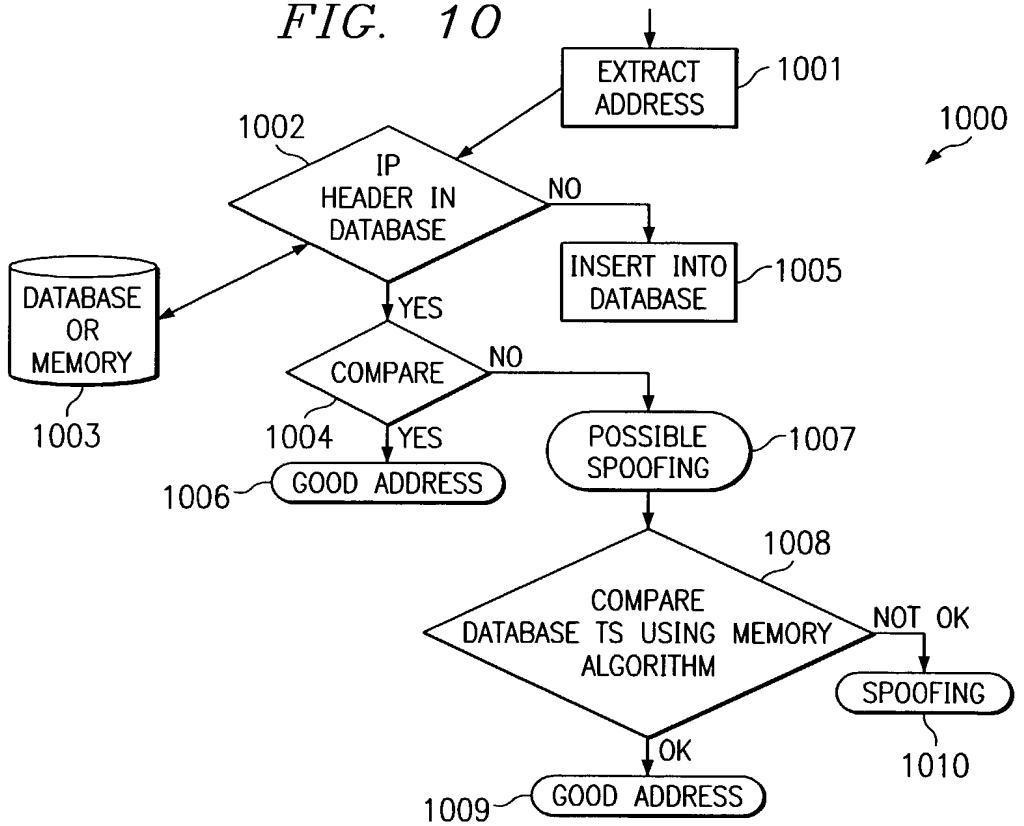

901
EXTRACT IP AND HARDWARE ADDRESS
902
SEARCH NETWORK
900
903
DNS INTERNET MATCH
NO
SEARCH LOCAL
904
YES
906
IP DOMAIN
DATABASE OR MEMORY
905
908
YES
MATCH
YES
MISMATCH
910
NO
909
910
907
GOOD IP ADDRESS
INDETERMINATE
INDETERMINATE
SPOOFING
911

FIG. 10


EXTRACT ADDRESS
1001
1000
1002
IP HEADER IN DATABASE
NO
INSERT INTO DATABASE
1005
DATABASE OR MEMORY
YES
COMPARE
NO
1003
1004
YES
POSSIBLE SPOOFING
1007
1006
GOOD ADDRESS
1008
COMPARE DATABASE TS USING MEMORY ALGORITHM
NOT OK
SPOOFING
1010
OK
1009
GOOD ADDRESS